PATIENT CONSENT, SENSITIVE DATA AND HEALTH INFORMATION EXCHANGE

by Helen Oscislawski, Esq.

Patient consent is one of the most passionately debated, hot button issues with electronic health information exchange (HIE). The crux of the tension lies, in part, between the need to make pertinent health information more readily accessible to the patient's treating physicians, and the patient's desire to control and keep such information private. On the one hand, if technology is used to move information out of its "paper record-silo" and into the hands of the decision-making clinicians, this can increase efficiency, reduce costs, and ultimately result in overall better medical care delivered to the patient. On the other hand, patients who seek medical treatment have certain expectations that their information will be kept confidential and may not want to have all of their health information available to all of their physicians.

The complex web of issues that patient consent and related privacy rights raise in the HIE context are intertwined with legal, technical and operational considerations. This article provides an overview of certain challenges that networked HIE presents, as well takes a brief look at certain technological solutions that may better protect sensitive data and afford patients with greater control with HIE. Readers should always consult with their own attorneys, however, before sharing patient information through any HIE network.

Consent Options for Health Information Exchange

A March 2010 whitepaper on patient consent options prepared by the Department of Health Policy, School of Public Health and Health Services at George Washington University Medical Center (the "GWU Consent Whitepaper") found that five (5) prevailing models have surfaced for HIE: (1) "*No Consent*" (2) "*Opt-Out*" (3) "*Opt-Out, with granularity of choice*" (4) "*Opt-In*" and (5) "*Opt-In, with granularity of choice*".[1] These five models are described in detail in the GWU Consent Whitepaper.

As between Opt-In, Opt-Out and No Consent, the Opt-Out consent model has certain advantages. First, it continues to protect patients' privacy by giving patients the right to make *a choice* about whether to allow providers to access their health information electronically for certain pre-defined permitted purposes (i.e., treatment). That is, if the patient does not want to allow his/her physicians to gain access to his/her aggregated medical information, the patient can choose to "opt-out" of participating in networked HIE. Second, the approach allows for a more complete clinical record to be created about the patient sooner, which the physician then has the opportunity to view before administering medical treatment. Physicians have indicated that if significant components of the patient's health information record are missing or incomplete, this makes the data found in an HIE network potentially less reliable and valuable from a clinical decision-making standpoint. Finally, from an administrative perspective, the Opt-Out approach is said to be somewhat less cumbersome to implement than, for instance, the Opt-In approach, or any approach affording granularity of choice.

---

[1] *Consumer Consent Options for Electronic Health Information Exchange: Policy Consideration and Analysis* (March 23, 2010).

The Opt-Out approach is also well documented in research papers and environmental scans as an acceptable consent model for HIE. Of the nine (9) states evaluated in the GWU Consent Whitepaper, three (3) (Virginia, Tennessee, and Maryland) adopted an Opt-Out approach to patient participation for their respective state exchanges, and two (2) (Delaware and Indiana) adopted the "No Consent" approach, which affords patients with *even less* choice with regard to whether or not their information will be shared through an HIE.[2] In addition, a recent scan of all fifty (50) states revealed that twenty-two (22) states have introduced and/or passed legislation that addresses patient consent specifically with regard in the networked HIE environment.[3] Of those twenty-two, sixteen (16) have introduced and/or enacted legislation that supports an Opt-Out approach. In those states where specific HIE standards have not been legislated, many initiatives have nevertheless decided to proceed with an Opt-Out approach.

On the other side of the HIE consent "coin," with the Opt-In approach, the patient's written consent is obtained *before* any information is shared for specific purposes. Some initiatives also require the patient's consent before any demographic information is disclosed to a third party vendor in connection with HIE, even for purposes such as creating a master patient index. In any case, typically no data is released from its originating "location" or shared with any other HIE-participating provider *until* the patient has affirmatively signed a written consent form agreeing to specific activities. This is believed to afford patients with maximum control over how their information is shared, and who is permitted to view their information.

Collecting a signed written consent is an appropriate endpoint to a process of educating patients about the benefits and inherent risks associated with electronic HIE. It also can ensure that patients have made an informed decision choice about allowing their information should be stored and shared through an electronic HIE network. However, implementing processes for effectively managing written consents can be challenging. In some cases, the entity overseeing the HIE activities (i.e., the health information organization (HIO)) may help manage these consents; however, if such centralized, coordinated consent management is not available, then the responsibility will usually fall on the shoulders of the providers. In addition, while some may believe that consent management begins and ends with obtaining the initial signed form, this is not the case. Managing Opt-In consents includes processing a patient's revocation of consent, as well as reversals of such revocations, as well as updating consents after they expire. Also, if the written consent covers only certain specific uses and disclosures set forth in a signed consent (i.e., for treatment), if the HIE initiative needs to use data for any other purpose, it would need to update and obtain resigned consents from all patients *before* moving forward.

The Office of National Coordinator (ONC)'s Privacy and Security Tiger Team ("Privacy Tiger Team") recognized that both Opt-In and Opt-Out, and their more granular counterparts, are each a potentially acceptable consent approaches for HIE, provided that the process implemented to effectuate the adopted approach complies with applicable law and affords the patient with an opportunity to exercise "*meaningful choice*". In order to better ensure that patients understand their options with regard to participating in or "opting out" of HIE, the Privacy Tiger Team

---

[2] See GWU Consent Whitepaper. (*Note that 4 states adopted Opt-In: Massachusetts, New York, Rhode Island, and Washington*).

[3] Attorneys at Oscislawski LLC, *50-State Legal Scan of Health Information Exchange Legislation* (September 2011).

recommended that participants engaging in HIE prepare and disseminate a layered Notice of Privacy Practices (NPP) that includes at least a short summary of electronic HIE policies, and with a more detailed notice to be made available for interested patients.

In the end, the decision whether to adopt an Opt-Out or Opt-In consent model (or any one of the other more granular counterparts) must take into consideration the circumstances and goals of the particular HIE network. The consent model selected will subsequently affect what ***types of participants*** may join the HIE network without first having to obtain additional specific written consent from their patients to disclose/share health information to or through the HIE network. Whether a particular type of participant will be allowed under applicable law to share information with the HIE network may then, in turn, be affected by the ***"permitted purposes"*** for which the network allows patient information to be accessed and used (e.g., treatment only, or will there be other uses?), and what ***type of information*** will automatically be included in and shared through the HIE network (i.e., demographic information only? sensitive information? de-identified information?). Finally, if and how the selected HIE technology can (*or cannot*) support identification and segmentation of "sensitive participants" or "sensitive data" will also affect whether the particular consent approach can be implemented in compliance with the law.

Federal and State Law Considerations

As of the date of this article, there continues to be no federal law that *specifically* governs networked electronic HIE. Therefore, most HIE consent models have been structured around the legal parameters set forth in the Health Insurance Portability and Accountability Act of 1996 and its related Privacy Rule and Security Rule (collectively "HIPAA"), the Health Information Technology for Economic and Clinical Health Act and its related rules (collectively "HITECH"), and other applicable federal and state privacy laws governing patient information.

With regard to sharing of information between health care providers ***for treatment*** purposes, HIPAA does not require an individual's prior written authorization or consent. The so-called "treatment exception" was carved out by HIPAA in order to prevent disruption of firmly established workflows and referral activities between providers. However, HITECH has created certain additional protections and rights with regard to patient information. For example, Section 13424(d) of HITECH requires:

> "[N]ot later than one year after the date of the enactment of this title, the Comptroller General of the United States shall submit [….] **a report** on the **best practices related to the disclosure** among health care providers of protected health information of an individual for purposes of treatment of such individual. Such **report shall include** an examination of the **best practices** implemented by States and by other entities, such as **health information exchanges** and **regional health information organizations**, an examination of the extent to which such best practices are successful with respect to the quality of the resulting health care provided to the individual and with respect to the ability of the health care provider to manage such best practices, and an **examination of the use of electronic informed consent** for disclosing protected health information for treatment, payment, and health care operations." (emphasis added).

In addition, Section 13424(f) of HITECH requires the Secretary (of HHS) to study the definition of ''**psychotherapy notes''** currently set forth in the HIPAA Privacy Rule and determine whether the same should be revised to include test data that is related to direct responses, scores, items, forms, protocols, manuals, or other materials that are part of a mental health evaluation, as determined by the mental health professional providing treatment or evaluation. Based on such study, HHS is charged with also making a recommendation as to whether to issue regulations to revise such definition, presumably to broaden the type of mental health-related information that would be afforded additional protection (i.e., require prior written authorization from the patient before being disclosed from its source).

Finally, Section 3002(2)(B) of HITECH directs the HIT Policy Committee:

> "[t]o make recommendations for . . . **[t]echnologies** that protect the privacy of health information and promote security in a qualified electronic health record, **including for the segmentation** and protection from disclosure of **specific and sensitive** individually identifiable health information *with the goal of minimizing the reluctance of patients to seek care* (or disclose information about a condition) *because of privacy concerns*, in accordance with applicable law, and for the use and disclosure of limited data sets of such information." (emphasis added).

The statutory provision also directs the HIT Policy Committee to make sure that the relevant and available recommendations and comments from the National Committee on Vital and Health Statistics (NCVHS) are considered in the development of its policies (*see* discussion on this topic further in this article).

New Jersey does not have a broad sweeping health information privacy law. Instead, patients' privacy rights with regard to their health information are addressed through a patchwork of statutes, regulations, and some case law. Generally, these laws can be grouped or categorized as follows:

- *Facility*-specific laws (e.g., hospitals; ambulatory care facilities; labs etc.)
- *Provider*-specific laws (e.g., physicians; nurses; pharmacists; psychologists etc.)
- *Sensitive Information* laws (e.g., HIV/AIDS; Genetic Information; STDs etc.)
- *Government Program*-specific laws (e.g., Medicaid; Family Planning etc.)

As a result of there being no overarching state privacy law that applies to all health information, the standards that govern how health information can be used and disclosed vary. For example, rules governing New Jersey licensed acute care hospitals require "*patient approval*" before information in the patient's records can be released, unless another healthcare care facility to which the patient was transferred requests the information, or the release of information is required and permitted by law, a third party payment contract, a medical peer review or the New Jersey State Department of Health. *See N.J.A.C.* 8:43G-4.1(a)21. However, the Board of Medical Examiner rules governing New Jersey licensed medical practitioners and their medical practices allow for exceptions in confidentiality, even in the absence of the patient's request, in cases where another licensed health care professional who is providing or has been asked to provide treatment to the patient. *See N.J.A.C.* 13:35-6.5(d)3.

The effect of this is that New Jersey law would permit certain providers to participate in an HIE network and share information for *treatment* purposes (with certain restrictions on sharing sensitive information, as discussed in the next section) pursuant to an Opt-Out approach without having to obtain any specific prior written consent of the patient; but, certain other providers would not be allowed under New Jersey law to share patient information with other participants through an HIE network, even for treatment purposes, unless specific prior written consent from the patient is obtained. Examples of restricted providers include mental health facilities, drug and alcohol rehabilitation facilities (including 42 CFR Part 2 providers), New Jersey Department of Health and Senior Services' local health agency providers, psychologists, family therapists, and social workers.

In addition to restricted provider types, information that is subject to additional protections under federal and/or state law (a.k.a. "Sensitive Information") almost always requires the patient's prior written consent before being disclosed. Certain federal or state law protections "attach to" such Sensitive Information and follow it downstream so that prior written consent would need to be obtained by the subsequent "custodian" of that information before it is re-disclosed again. Therefore, if Sensitive Information appears anywhere in the data shared through the HIE network, it can only be disclosed and accessed after all requirements under the applicable federal and state laws are met. The following are examples of categories of Sensitive Information specifically protected by federal and New Jersey law and that must be protected from access or use, unless specific requirements have been met:

- 42 CFR Part 2 Records;
- Genetic Information and Nondisclosure Act;
- Services paid for "out of pocket" (HITECH);
- Psychotherapy Notes (HIPAA);
- HIV/AIDS Information (N.J.S.A. 26:5C-8);
- Venereal Diseases (N.J.S.A. 26:4-41);
- Drug & Alcohol Rehabilitation Information (N.J.S.A. 26:2B-8);
- Mental Health Rehabilitation (N.J.A.C 10:37-6.79);
- Genetic Privacy Act of New Jersey (N.J.S.A. 10:5-43);
- Minor's Emancipated Treatment (N.J.S.A. 9:17B-1); and
- Social Security Numbers.

In addition, federal policy may move to require certain additional categories of information be treated as Sensitive Information. The NCVHS heard extensive testimony about the definitions of sensitive categories of health information beyond those that are currently recognized and protected under federal law. On November 14, 2010, NCVHS issued its *"Recommendations Regarding Sensitive Health Information*" to the Department of Health and Human Services. The NCVHS Recommendations suggest the following additional categories of information should potentially be treated as Sensitive Information in the HIE context:

- The following specific **Mental Health Information**[4]:

[4] Note, NCVHS excluded the following information from its definition of "sensitive" Mental Health Information: **medication lists; allergies and non-allergic drug interactions; dangerous behavior within medical settings; and information from**

- Psychiatric diagnoses
- Descriptions by patients of traumatic events
- Descriptions or analysis or reports by the patients of emotional, perceptual, behavioral, or cognitive states

- The following specific **Sexuality and Reproductive Health Information:**
  - Sexual activity
  - Sexual orientation
  - Gender dysphoria and sexual reassignment
  - Abortion, miscarriage, or past pregnancy
  - Infertility and use of assisted reproduction technologies
  - Sexual dysfunction
  - The fact of having adopted children

Therefore, it is important to recognize that not all information may be considered "equal". Indeed, many believe that general clinical information, such as patient allergies, medication lists, and diagnostic reports, should not be prevented from sharing among treating physicians. Yet, most HIE initiatives continue to struggle with how to adequately protect Sensitive Information but not bring all beneficial HIE to a standstill.

Segmentation, Sequestration, and Patient-Controlled PHRs

If a "restricted provider" type is looking to potentially disclose data through an HIE network, the provider usually can be flagged as a "Opt-In" provider and technology can be configured so that no data is ever automatically pulled, queried or accessed from such restricted provider until and unless the patient has specifically consented to such restricted provider sharing the patient's data with other providers. Sensitive Information, however, is not as easily handled, particularly when Opt-Out has been selected as a baseline approach.

Where federal and state law permits general clinical data to be shared without the patient's specific written authorization or prior consent, such information can be access by authorized providers in accordance with executed participation agreements, HIE policies and applicable laws. However, where Sensitive Information is embedded in the general data to be accessed, as is often the case with discharge summaries and other reports, the Opt-Out approach can present a problem because it is not possible to identify such Sensitive Information and prevent access based solely on administrative or manual processes. In light of this, many HIE initiatives move toward asking patients to sign a comprehensive "catch all" consent form that leaves the patient with no choice other than to consent to share all Sensitive Information if they wish to participate in the HIE network. However, more and more HIE initiatives are beginning to look to technological solutions to address the issue Sensitive Information presents for HIE.

---

medical notes, test, procedures, imaging or laboratory studies performed in a mental health facility that is not related to the mental health treatment but that would otherwise be considered medical information, such as cardiac studies to diagnose reported chest pain.

Some HIE initiatives are testing "plug in" software that scans data stored in the HIE repository and "tags" (or "segments") it when certain terms are found that correspond to rules developed around state and federal laws restricting access to such Sensitive Information. Once identified, the tagged data element, or document if it is not a discrete data segment, is removed from viewing, but a "flag" is shown so that the physician is made aware that the patient's electronic record contains "hidden" (or "sequestered") data that requires the patient's affirmative consent to be obtained before it can be viewed. Other HIE initiatives are addressing Sensitive Information by offering patient-controlled consent solutions as part of a personal health record (PHR) option. With this option, patients have the choice to "take charge" of controlling who can view or not view their Sensitive Information (as well as other data) by claiming their PHR account and managing their own consent preferences with regard to their information.

Using specialized technology to manage Sensitive Information attempts to move HIE forward with a balanced approach. Both data segmentation/sequestration technology and PHR solutions offer potential new approaches to an old problem. The anticipated and hoped for end result will be a compromise that gives physicians access to valuable information that will improve the delivery of care to patients and at the same time respects patients' privacy rights and desire to control access to certain information.